

REMARKS / ARGUMENTS

By this Amendment, Applicants respond to the Office Action dated April 28, 2005 ("the Office Action"), in which claims 1-20 were rejected. With this Amendment, Applicants have amended claims 1, 4-6, 18, and 19, and no new claims have been added. Accordingly claims 1-20 remain pending in this application.

Applicants respectfully request entry of the amendments indicated above to improve readability and to correct some minor typographical errors. Support for the amendments can be found in the application as filed. It will be appreciated that these amendments have been made for purposes of readability and clarity, not for purposes of patentability.

Rejection of Claims 1, 2, 4-6, 8-10, 14, 16 and 17 under 35 U.S.C. § 103(a)

Claims 1, 2, 4-6, 8-10, 14, 16 and 17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,064,739 to Davis ("Davis") in view of U.S. Patent No. 6,088,801 to Grecsek ("Grecsek"). These rejections are traversed respectfully in view of the following remarks.

Claims 1 and 2 recite methods for protecting electronic content from unauthorized use by a user of a computer system including the unique combination of receiving a request from a user of the computer system to access a piece of electronic content; identifying one or more software modules responsible for processing the piece of electronic content; evaluating one or more predefined characteristics of the one or more software modules; and denying the request to access the piece of

electronic content if the one or more predefined characteristics fail to satisfy a set of predefined criteria.

As Applicants noted in the Response and Amendment filed January 4, 2005, and the Examiner agreed in the Office Action, "Davis does not explicitly disclose identifying one or more software modules responsible for processing the piece of electronic content; evaluating one or more predefined characteristics of the one or more software modules; [and] denying the request ... if the one or more predefined characteristics fail to satisfy a set of predefined criteria." Office Action at ¶ 4. Instead, the Examiner asserts that Grecsek would have provided the necessary teachings and motivation to one of ordinary skill in the art to achieve the results of the claimed invention:

Grecsek discloses evaluate [sic] the risks of executing software processes based on capability-based policy to prevent unauthorized invocations of services located on the user's computer in order to protect data from unauthorized use (Grecsek: column 1 line 19 - column 2 line 47 and column 3 lines 17-51). Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Grecsek within the system of Davis because it increases data protection by making sure the data is not being used by unauthorized software hidden in the computer system.

Office Action at 2-3.

Applicants respectfully note that M.P.E.P. § 2142 puts forth the requirement, long settled by the Federal Circuit, that it is the Examiner's burden to provide a *prima facie* rejection for obviousness by demonstrating reasonably that: (1) there is some suggestion or motivation, either in the cited references or in the knowledge generally available to one of ordinary skill in the art, to modify or combine teachings to produce

the claimed invention; (2) there must be a reasonable expectation of success in achieving the claimed invention; and (3) the cited references must teach or suggest all the claim limitations in combination. M.P.E.P. § 2142. Use of Applicants' disclosure is forbidden. *Id.* The mere fact that the references *can* be combined is not sufficient to establish a *prima facie* rejection. *Id.* at § 2143.01. Moreover, the combination proposed by the Examiner cannot render the prior art unsatisfactory for its intended purpose or change the principle of operation described in a reference. *Id.*

Applicants respectfully submit that the Examiner has failed to provide a *prima facie* rejection of claims 1 and 2. First, Applicants note that the Examiner has not provided a reasonable basis for these rejections as set forth in elements (1)–(3) from M.P.E.P. § 2142 recited above. Rather, the Examiner has merely opined “that it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Grecsek within the system of Davis because it increases data protection by making sure the data is not being used by unauthorized software hidden in the computer system.” Applicants respectfully submit that this statement is conclusory, as it fails to provide any rationale concerning the requisite elements of motivation, expectation of success, and teaching of all claim elements. Applicants thus respectfully submit that the Examiner has not met the burden of providing *prima facie* rejections, and request that the rejections be withdrawn.

Applicants further respectfully suggest that the rationale necessary to make a *prima facie* rejection is not possible. Applicants respectfully note that the Examiner's combination of Davis and Grecsek would violate the requirements of M.P.E.P. § 2143.01, as such a combination would render each of the cited references unsatisfactory for its intended purpose. Davis describes protecting video data from unauthorized copying using a first encryption engine to decrypt previously encrypted video data and re-encrypt that data, a frame buffer to store the newly encrypted video data, and a second encryption engine to decrypt the video data in the frame buffer prior to transmission to an analog signal for display. Davis at Column 2, lines 19–29. The components are encased in a hardware envelope that prevents interception of the decrypted video data. *Id.* at lines 63–65.

Grecsek describes systems and methods for identifying malicious software code before the code is executed on a computer system. Grecsek at Column 2, lines 40–45. The systems and methods described in Grecsek “provide a means for determining the capabilities of [a potentially malicious] process ... before it executes.” *Id.* at lines 23–27. A process that is determined to include potentially dangerous operations can be denied access to system resources or have certain operations disabled. See, Column 4, lines 21–36.

Applicants note that one of ordinary skill in the art would not have any motivation to combine Davis with Grecsek without the use of prohibited hindsight, since the two references address different problems and operate on different types of data. Davis is concerned with copy protection; not preventing the execution of

malicious operations. The methods and systems described by Grecsek are directed to evaluating program operations, and do not address securing data using an encryption-decryption scheme within a separate hardware device. Conversely, the encryption-decryption methods and systems described in Davis do not relate to identifying malicious code and preventing the execution of such code. The Examiner has not presented any argument or evidence to explain why or how one of ordinary skill would combine these two very different descriptions to obtain the invention as claimed.

But assuming *arguendo* that the references could be combined within the requirements of M.P.E.P. §§ 2142 and 2143, Grecsek still does not overcome the admitted deficiencies of Davis. Grecsek describes evaluating processes prior to their execution, and modifying the execution of such processes if certain criteria are met. In particular, Grecsek does not show or suggest the unique combination of receiving a request for electronic content, identifying software modules responsible for processing that content, evaluating those modules, and denying a request for access to electronic content if one or more predefined characteristics of identified software modules fail to satisfy a set of predefined criteria. Again, those details can only be provided using Applicants' invention. In particular, Grecsek apparently evaluates all code without regard to any particular content to be processed.

Thus, Applicants can only understand that the Examiner has appealed to prohibited hindsight in asserting this combination; and respectfully request that the Examiner withdraw the outstanding rejections.

Claim 4 recites a system for protecting electronic content comprising the unique combination of:

- means for applying a cryptographic fingerprint to the electronic content;
- means for evaluating one or more predefined characteristics of the drivers responsible for handling the electronic content;
- means for denying effective access to the electronic content based on an output of said means for evaluating one or more predefined characteristics of the drivers responsible for handling the electronic content;
- means for generating an identifier associated with the electronic content;
- means for monitoring a predefined system interface for data containing the identifier; and
- means for preventing effective access to data containing the identifier via the predefined system interface.

Neither Davis nor Grecsek, alone or in combination, shows or suggests the use of an electronic fingerprint as claimed. Thus, the cited prior art does not render claim 4 obvious. Applicants respectfully request that the Examiner withdraw this rejection.

Claims 5–20 recite a method for protecting electronic content from unauthorized use comprising:

- receiving a request to access a piece of electronic content;
- generating a first identifier associated with the electronic content;

monitoring at least one system interface, the monitoring including:

receiving a piece of electronic data;

generating a second identifier associated with the piece of
electronic data;

comparing the second identifier with the first identifier;

taking a predefined defensive action if the second identifier is
related to the first identifier in a predefined manner.

Neither Davis nor Grecsek, alone or in combination, shows or suggests generating a first identifier as claimed. Thus, the cited prior art does not render claims 5–20 obvious. Applicants respectfully request that the Examiner withdraw these rejections.

Rejection of Claims 3, 7, 15, and 18-20 under 35 U.S.C. § 103(a)

Claims 3, 7, 15, and 18-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Davis in view of Grecsek and further in view of U.S. Patent No. 5,745,678 to Herzberg et al. ("Herzberg"). These rejections are respectfully traversed in view of the following remarks.

Each of the rejected claims depends from claims 1 or 5. As noted above, the combination of Davis and Grecsek does not show or suggest the unique combinations of those claims. The Examiner cites Herzberg as disclosing "using [a] cryptographic hash value to authenticate whether a software program is authorized (Herzberg: column 1 line 44–column 2 line 35)." Office Action at 7. The Examiner asserts that "[i]t would have been obvious to one having ordinary skill in the art at the time of

applicant's invention to combine the teachings of Herzberg within the combination of Davis-Grecsek because it is well known in the art to authenticate whether an object is authorized for access using cryptographic hash." *Id.* at 7.

However, the combination of Davis and Herzberg is inconsistent with the purpose of Davis. Davis is not concerned with the authenticity of software programs. Davis discloses methods and apparatus for preventing unauthorized copying of video data. There is no need to authenticate the video data in Davis, since that data is understood to be valid (which is why someone might want to copy that data).

The combination of Grecsek and Herzberg also would pervert the rationale of the references. Grecsek teaches the evaluation of software programs to identify operations that could compromise the user's computer. Grecsek does not show or suggest using hashes to determine the integrity of the code itself. Indeed, Grecsek actually teaches away from using cryptographic methods to secure software:

Cryptography techniques insure that messages are protected during transmission. Yet, they offer no protection after messages are received, which can include unauthorized invocations of services located on the user's computer. Authentication techniques do not address the problem because risk must ultimately be determined by each user based on their own unique context. Acceptable risk for one user may not be acceptable for another. Moreover, once a user authorizes an authenticated process for a particular purpose, there is nothing to prevent other unrelated processes from using the methods of the authenticated process in an unauthorized manner.

Grecsek at Column 1, lines 50–61. Thus, the methods disclosed by Grecsek would not lead one of ordinary skill to combine the methods disclosed in Herzberg, as that combination would not further the purpose of Grecsek to evaluate potentially malicious software.

Furthermore, the rejected claims each require at least the unique elements of generating first and second identifiers, comparing those identifiers, and taking a predetermined action if the first and second identifiers are different. None of the cited prior art, either alone or in combination, shows or suggests these elements. Applicants therefore respectfully request that the Examiner withdraw the rejections.

Rejection of Claim 11 under 35 U.S.C. § 103(a)

Claim 11 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Davis in view of Grecsek and further in view of U.S. Patent No. 6,236,727 to Ciacelli et al ("Ciacelli"). This rejection is respectfully traversed in view of the following remarks.

The Examiner asserts that "Ciacelli discloses scrambling portion of electronic data to protect copyright data (Ciacelli: column 2 lines 3-65)." Office Action at 9. The Examiner concludes, without any supporting argument or evidence, that "[it] would have been obvious to one having ordinary skill in the art at the time of invention to combine the teachings of Ciacelli within the combination of Davis-Grecsek because scrambling a digital data protects the data from being viewed or used by unauthorized parties."

Applicants respectfully submit that Ciacelli does nothing to address the above-enumerated differences of Davis and Grecsek. In fact, Ciacelli describes an apparatus and method very similar to that described in Davis:

Generally stated, the present invention comprises an apparatus, method and computer program product for processing a data stream scrambled, for example, by employing content scrambling system (CSS) technology. As one aspect, the invention comprises descrambling a received CSS encrypted signal at a central

processing unit without subsequently exposing a clear copy of the descrambled data in any accessible structure outside the CPU, such as memory or a system bus. This insures that information to be protected, such as security data or copyrighted material (herein collectively referred to as "copyright data"), will not be exposed at a point where illegal copying of the original data stream is feasible (e.g., during data transfer) while still allowing software descrambling of the CSS encrypted stream.

Ciacelli at Column 3, lines 25–40. Thus, Ciacelli does not teach the scrambling of data as suggested by the Examiner. Rather, Ciacelli teaches methods for *descrambling* and decrypting data without exposing the unscrambled (unencrypted) data to copying. Moreover, combining Ciacelli and Grecsek would defeat the objectives of each of those teachings for the reasons discussed above regarding Davis and Grecsek. Thus, the combination of Davis, Grecsek, and Ciacelli cannot be said to render the invention obvious. Applicants respectfully request that the Examiner withdraw this rejection.

Rejection of Claims 12 and 13 under 35 U.S.C. § 103(a)

Claims 12 and 13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Davis in view of Grecsek and further in view of European Patent No. EP0915620 to Shimada ("Shimada). However, claims 12 and 13 are dependent on claim 5, and are thus patentable for at least the reasons set forth above in connection with claim 5. Applicants therefore respectfully request that the Examiner withdraw these rejections.

Appln. No. 09/653,517
Amdt/Rsp filed Oct. 28, 2005 with RCE
replying to Office Action mailed April 28, 2005

PATENT
Customer No. 22,852
Attorney Docket No. 7451.0029-00
InterTrust Ref. No. IT-28.1

CONCLUSION

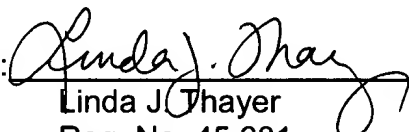
In view of the foregoing remarks, Applicants submit that the pending claims are in allowable form, and respectfully request reconsideration of the rejections and timely allowance of the claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: October 27, 2005

By: 
Linda J. Thayer
Reg. No. 45,681

Finnegan, Henderson, Farabow
Garrett & Dunner, L.L.P.
1300 I Street, NW
Washington, D.C. 20005
(202) 408-4000

AMENDMENTS TO THE DRAWINGS:

The drawings as filed were accepted by the Office, and Applicants submit these replacement sheets solely so that the Office will have a cleaner copy. The drawings have not been amended and therefore contain no new matter.

Attachments: 8 Replacement Sheets of Drawings (Figs. 1-8)